IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

KATHARINE UHRICH, PLAINTIFF, **v.** **TEACHERS INSURANCE AND ANNUITY ASSOCIATION OF AMERICA,** DEFENDANT.	Case No.

<u>CLASS ACTION COMPLAINT</u>

Plaintiff Katharine Uhrich, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant Teachers Insurance and Annuity Association of America ("TIAA" or "Defendant"), to seek redress for the Defendant's conduct leading up to, surrounding, and following a data vulnerability and breach incident that exposed the personal information of hundreds of thousands of their customers. Plaintiff alleges as follows upon personal knowledge as to themselves and their own acts and experiences, and as to all other matters, upon information and belief, including an investigation conducted by their attorneys.

<u>NATURE OF CASE</u>

1. Defendant TIAA is a New York based insurance and financial service company that operates in all 50 states, including the state of Illinois.

2. TIAA failed to safeguard the confidential personal identifying information of the Plaintiff and numerous other individuals ("Class Members" or

collectively as the "Class"). This class action is brought on behalf of Class Members whose personally identifiable information ("PII", or "Private Information") was accessed sensitive information through the Defendant's computer system without the Plaintiff permission or knowledge.

3. TIAA's failure to implement or maintain adequate data security measures for personal information directly and proximately caused injuries to Plaintiff and the Class.

4. TIAA failed to take reasonable steps to employ adequate security measures or to properly protect sensitive PII despite well-publicized data breaches at numerous businesses and financial institutions in recent years.

5. Despite numerous and high-profile data breaches, TIAA failed to implement basic security measures to prevent unauthorized access to this information.

6. Citizens from across Illinois and the United States have suffered real and imminent harm as a direct consequence of the Defendant's conduct, which includes: (a) refusing to take adequate and reasonable measures to ensure its data systems, as well as the data stored therein, were protected; (b) refusing to take available steps to prevent the breach from happening; (c) failing to disclose to its customers the material facts that it did not have adequate computer systems and security practices to safeguard Private Information; and (d) failing to provide timely and adequate notice of the data breach.

7. The Data Breach was the inevitable result of TIAA's inadequate data security measures and approach to data security. Despite the well-publicized and ever-growing threat of security breaches, and even though data breaches were and are occurring across numerous industries, Defendant failed to ensure that they maintained adequate data security measures causing the Private Information of Plaintiff and Class Members to be stolen.

8. As a direct and proximate consequence of TIAA's negligence, a massive amount of customer information was stolen from TIAA. Victims of the Data Breach have had their Private Information compromised, had their privacy rights violated, been exposed to the increased risk of fraud and identify theft, lost control over their personal and financial information, and otherwise been injured.

9. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address TIAA's inadequate safeguarding of Class Members' Private Information that they collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access of an unknown third party.

JURISDICTION AND VENUE

10. This Court has jurisdiction over this case pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because members of the proposed Classes are citizens of states in the United States and the foreign Defendant are subjects or citizens of foreign states, and the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs.

11. This Court has supplemental jurisdiction over Plaintiff's state law claims under 28 U.S.C. § 1367.

12. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because a substantial part of the events, omissions, and acts giving rise to the claim occurred in this District. Moreover, Plaintiff resides in this District.

PARTIES

13. Plaintiff Katharine Uhrich ("Plaintiff" or "Ms. Uhrich") was a resident and citizen of Illinois during all times relevant to this complaint.

14. Plaintiff used Defendant as a retirement service provider when working for her former employer. Plaintiff provided Defendant with her personal information in order to create and maintain an account with Defendant, and trusted Defendant to maintain her personal information in a safe and secure manner.

15. Plaintiff became aware that her PII had been involved in a data breach of Defendant when she received a letter dated July 25, 2023. (Exhibit A, Data Breach Letter).

16. Defendant TIAA Services, Inc. is a corporation organized under the laws of New York, with its principal place of business located in New York.

FACTUAL ALLEGATIONS

A. The Data Breach

17. Defendant obtained significant Personal Information on consumers throughout the United States, including that of Plaintiff and the Class Members, as a result of its business operations.

18. On or around July 14, 2023, Defendant announced that it had previously, on or about May 31, 2023, suffered a data breach that impacted millions of individuals.

19. Plaintiff's and Class Members' sensitive personal information, which was entrusted to the Defendant, its officials and agents, was compromised, unlawfully accessed, and stolen due to the data breach.

20. On information and belief, at minimum, significant personally identifiable information was included in the data breach:

A. Name;

B. Social Security number;

C. Gender;

D. Date of birth;

E. Address.

21. As a result of Defendant's actions and/or inaction, Plaintiff and the Class Members were harmed and must now take remedial steps to protect themselves from future loss. Indeed, Plaintiff and all Class Members are currently at a very high risk of misuse of their Private Information in the coming months and years, including but not limited to unauthorized account access including on third-party services and identity theft through use of personal information to open up accounts.

22. As a result of TIAA's failure to properly and timely notify their customers of the full extent of the data breach, members of the class have not had the opportunity to fully protect themselves and take any specific precautions.

23. The unauthorized access occurred because third parties were able to access Plaintiff's and the Class's personal information because Defendant failed to take reasonable measures to protect the Private Information it collected and stored. Among other things, Defendant failed to implement data security measures designed to prevent this attack, despite repeated industry wide warnings about the risk of cyberattacks and the highly publicized occurrence of many similar attacks in the recent past.

24. As a result of TIAA's failure to properly secure Plaintiff's and the Class Members' personal identifying information, Plaintiff's and the Class Members' privacy has been invaded.

25. Moreover, all of this personal information is likely for sale to criminals on the dark web, meaning that unauthorized parties have likely accessed and viewed Plaintiff's and the Class Members' PII.

B. Data Breaches and Industry Standards of Protection of PII

26. Identity theft, which costs Americans billions of dollars a year, occurs when an individual's personal identifying information is used without his or her permission to commit fraud or other crimes. Victims of identity theft typically lose hundreds of hours dealing with the crime, and they typically lose hundreds of dollars.

27. According to the Federal Trade Commission ("FTC"):

> **Identity theft is serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing**

> **or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.**

28. The United States Government Accountability Office ("GAO") has stated that identity thieves can use identifying data to open financial accounts and incur charges and credit in a person's name. As the GAO has stated, this type of identity theft is the most damaging because it may take some time for the victim to become aware of the theft and can cause significant harm to the victim's credit rating. Like the FTC, the GAO explained that victims of identity theft face "substantial costs and inconvenience repairing damage to their credit records," as well the damage to their "good name."

29. Industry Standards highlight several basic cybersecurity safeguards that can be implemented to improve cyber resilience that require a relatively small financial investment yet can have a major impact on an organization's cybersecurity posture including: (a) the proper encryption of Private Information; (b) educating and training employees on how to protect Private Information; and (c) correcting the configuration of software and network devices.

30. Identity theft crimes often encompass more than just immediate financial loss. Identity thieves often hold onto stolen personal and financial information for several years before using and/or selling the information to other identity thieves.

31. Accordingly, federal and state legislatures have passed laws to ensure companies protect the security of sensitive personally identifying confidential information, such as that wrongfully disclosed in the Data Breach.

32. The FTC has issued a publication entitled "Protecting Personal Information: A Guide for Business" ("FTC Report"). The FTC Report provides guidelines for businesses on how to develop a "sound data security plan" to protect against crimes of identity theft. To protect the personal sensitive information in their files, the FTC Report instructs businesses to follow, among other things, the following guidelines:

A. Know what personal information you have in your files and on your computers;
B. Keep only what you need for your business;
C. Protect the information that you keep;
D. Properly dispose of what you no longer need;
E. Control access to sensitive information by requiring that employees use "strong" passwords; tech security experts believe the longer the password, the better; and
F. Implement information disposal practices reasonable and appropriate to prevent an unauthorized access to personally identifying information.

33. The FTC Report also instructs companies that outsource any business functions to proactively investigate the data security practices of the outsourced company and examine their standards.

34. The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. See, e.g., *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

C. TIAA Failed to Prevent the Data Breach, Putting Plaintiff and Class Members at Risk

35. Upon information and belief, TIAA has policies and procedures in place regarding the safeguarding of confidential information they are entrusted with, and TIAA failed to comply with those policies.

36. TIAA also negligently failed to comply with industry standards or even implement rudimentary security practices, resulting in Plaintiff's and the Class's PII being substantially less safe than had this information been entrusted with other similar companies.

37. TIAA was aware of the likelihood and repercussions of cyber security threats, including data breaches, having doubtlessly observed numerous other well-publicized data breaches involving major corporations over the last decade- as well as the numerous other similar data breaches preceding those major breaches.

38. In addition to TIAA's failure to prevent the Data Breach, TIAA also failed to timely detect the Data Breach and realize this Private Information remained publicly accessible and unencrypted for a substantial amount of time.

39. Hackers, cyber-criminals, and other nefarious actors, therefore, had sufficient time to collect this Private Information unabated. During this time, TIAA

failed to recognize the failure to protect this Private Information. If TIAA had quickly detected the Data Breach, this likely would have significantly reduced the consequences of the Data Breach. Instead, TIAA's delay in detecting the Data Breach contributed to the scale of the Data Breach and the resulting damages.

40. The Data Breach occurred because TIAA failed to implement adequate data security measures to protect its database and computer systems from the potential dangers of a data breach and failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach.

41. The Data Breach was caused and enabled by TIAA's knowing violation of its obligations to abide by best practices and industry standards in protecting Private Information.

D. The Data Breach caused Current and Future Harm

42. As a direct and proximate result of TIAA's wrongful disclosure, criminals now have Plaintiff's and the Class Members' Private Information.

43. TIAA's wrongful actions and inactions here directly and proximately caused the public disclosure of Plaintiff's and Class Members' personal identifying information without their knowledge, authorization and/or consent. As a further direct and proximate result of TIAA's wrongful actions and/or inaction, Plaintiff and Class Members have suffered, and will continue to suffer, damages including, without limitation, expenses for credit monitoring and identity theft insurance, out-of-pocket

expenses, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm.

44. As a further result of the data breach, Plaintiff and Class Members have been exposed to a substantial and present risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

45. Identity thieves can use personal information, such as that of Plaintiff, the other Class Members, which TIAA's failed to keep secure, to perpetrate a variety of crimes that harm victims. Even basic personal information, combined with other contact information, is very valuable to hackers and identity thieves as it allows them to access users' other accounts. Thus, even if some information was not involved in the Data breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access other information, including, but not limited to email accounts, government services accounts, e-commerce accounts, payment card information, and financial accounts, to engage in the fraudulent activity identified by Plaintiff.

46. TIAA was at all times fully aware of its obligations to protect the Private Information of Plaintiff and Class Members. Plaintiff and Class Members would not have entrusted their Private Information to TIAA had they known that TIAA would fail to maintain adequate data security. TIAA was also aware of the significant repercussions that would result from their failure to do so.

47. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. Identity theft victims must spend numerous hours and their own money repairing the impact to their credit.

48. Thus, Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights.

49. TIAA's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff, the other Class members' Private Information, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including but not limited to:

a. Theft of their Private Information and financial information;

b. Costs for credit monitoring services; unauthorized charges on their debit and credit card accounts;

c. Unauthorized charges on their debit and credit cards;

d. Injury flowing from potential fraud and identity theft posed by their credit/debit card and Private Information being placed in the hands of criminals and already misused via the sale of Plaintiff and Class members' Private Information on the black market and dark web;

e. Losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

f. Losses in the form of deprivation of the value of their Private Information;

g. The untimely and inadequate notification of the Data Breach;

h. The improper disclosure of their Customer Data;

i. Loss of privacy;

j. Loss of use of, and access to, their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and,

k. The loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services.

50. Additionally, even with credit monitoring, the damages of a Data Breach will last much longer since this Private Information cannot be completely removed from the possession of cybercriminals. In fact, it will likely continue to circulate on the dark web and be sold or traded to other hackers and cybercriminals or identity thieves who will use it to continue to perpetuate fraud against the Class Members.

51. Although the Private Information of Plaintiff and the Class Members has been stolen, TIAA's continues to hold Private Information of the affected individuals, including Plaintiff and the Class Members.

52. Particularly, because TIAA has demonstrated an inability to prevent a data breach or stop it from continuing even after being detected and informed of the impermissible dissemination—Plaintiff, the other Class members, have an undeniable interest in ensuring their Private Information is secure, remains secure, is properly and promptly destroyed, and is not subject to further disclosure and theft.

53. Accordingly, Plaintiff on behalf of themself and the Class, bring this action against Defendant seeking redress for their unlawful conduct.

CLASS ALLEGATIONS

54. Plaintiff brings these claims on behalf of themselves and of the following classes pursuant to Federal Rule of Civil Procedure 23:

55. Plaintiff brings these claims on behalf of the following classes:

> **National Class: All individuals whose PII was exposed while in the possession of Defendant, or any of its subsidiaries and/or agents, during the Data Breach.**
>
> **Illinois Sub-Class: All individuals in Illinois whose PII was exposed while in the possession of Defendant, or any of their subsidiaries and/or agents, during the Data Breach.**

56. Excluded from the class are Defendant, its parents, subsidiaries, affiliates, officers, and directors, all persons who make a timely election to be excluded from the class, the judge to whom this case is assigned and any immediate family members thereof, and the attorneys who enter their appearance in this action.

57. Plaintiff may alter the class definitions to conform to developments in the case and discovery.

58. The proposed class meets all requirements under Fed. R. Civ. P. 23.

59. **Numerosity:** Upon information and belief, the Class is so numerous that joinder of all individual Plaintiff would be impracticable. The exact number of members of the Class is presently unknown and can only be ascertained through discovery because that information is exclusively in the possession of Defendant. However, it is reasonable to infer that more than 40 individuals in each class were impacted by the data breach at issue. Members of the Class can be easily identified through Defendant's records. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, Internet postings, and/or published notice.

60. **Commonality:** This action involves common questions of law and fact, which predominate over any questions affecting individual members of the Class, including, without limitation:

A. Whether Defendant negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and Class Members' personal identifying information;

B. Whether Defendant was negligent in storing and failing to adequately safeguard Plaintiff's and Class Members' personal identifying information;

C. Whether Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in protecting and securing their personal identifying information;

D. Whether Defendant breached their duties to exercise reasonable care in failing to protect and secure Plaintiff's and Class Members' personal identifying information;

E. Whether by disclosing Plaintiff's and Class Members' personal identifying information without authorization, Defendant invaded Plaintiff's and Class Members' privacy;

F. Whether Plaintiff and Class Members sustained damages as a result of Defendant's failure to secure and protect their personal identifying information.

61. **Typicality**: Plaintiff's claims are typical of the claims of the Class members, as they are all based on the same factual and legal theories. Plaintiff and all Class Members sustained damages arising out of and caused by the Defendant's common course of conduct in violation of law.

62. **Adequacy of Representation:** Plaintiff is an adequate representative of the Class because their interests do not conflict with the interests of the members of the Class they seek to represent, and they intend to prosecute this action vigorously. Plaintiff has retained counsel competent and experienced in consumer class actions and complex litigation. The interests of the Class will be fairly and

adequately protected by Plaintiff and their counsel and Plaintiff's claims are typical of the claims of the class members.

63. **Superiority:** A class action in this case would be appropriate and superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and members of the Class are relatively small compared to the burden and expense that would be required to individually litigate their claims against the Defendant, so it would be impracticable for members of the Class to individually seek redress for the Defendant's wrongful conduct. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the judicial system. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

64. **Ascertainability:** The class members are easily ascertainable from the Defendant's records and it would not be difficult to obtain this specific information in Discovery.

65. Defendant has acted or failed to act on grounds that apply generally to the class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

66. Class certification, therefore, is appropriate pursuant to Rule 23 because the above common questions of law or fact predominate over any questions affecting

individual Class Members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

COUNT I - NEGLIGENCE

(ON BEHALF OF PLAINTIFF AND THE CLASSES)

67. Plaintiff re-alleges the preceding paragraphs as is set forth fully in this Count.

68. Defendant obtained sensitive Private Information about Plaintiff and Class Members.

69. Upon Defendant's accepting and storing the Private Information of Plaintiff and the Class in its computer systems and on its networks, Defendant undertook and owed a duty to Plaintiff and the Class to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendant knew that the Private Information was private and confidential and should be protected as private and confidential.

70. Defendant owed a duty of care not to subject Plaintiff's and the Class Members' Private Information to an unreasonable risk of exposure because Plaintiff and the Class were foreseeable and probable victims of any inadequate security practices.

71. Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their PII in its possession from being compromised, lost, stolen, accessed or misused by unauthorized persons. More specifically, this duty included, among

other things: (a) designing, maintaining, and testing its security systems, as well as those of any third-party contractors, to ensure that Plaintiff's and Class Members; PII in Defendant's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

72. It was reasonably foreseeable that TIAA's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information would result in an unauthorized third-party gaining access to such information without Plaintiff's or Class Members' knowledge or consent.

73. Defendant knew, or should have known, of the risks inherent in collecting, storing, and sharing Private Information amongst themselves and the importance of adequate security. Defendant knew of should have known about numerous well-publicized data breaches within the industry.

74. Defendant's duty to use reasonable security measures also arose as a result of the special relationship that existed between Defendant, on the one hand, and Plaintiff and Class Members, on the other hand.

75. The special relationship arose because Plaintiff and Class Members entrusted Defendant with their PII as part of the applications or use of the Defendant's products and services. Defendant alone could have ensured that its

security systems and data storage architecture were sufficient to prevent or minimize the Data Breach.

76. Defendant's duty also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII by companies such as Defendant. Various FTC publications and data security breach orders further form the basis of Defendant's duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

77. Defendant also had a duty to safeguard the PII of Plaintiff and Class Members and to promptly notify them of a breach because of state laws and statutes that require Defendant to reasonably safeguard sensitive PII, as detailed herein.

78. Defendant breached the duties they owed to Plaintiff and Class Members described above and thus was negligent.

79. Defendant breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiff and Class Members; (b) immediately detect the Breach while it was ongoing; (c) maintain security systems consistent with industry standards during the period of the Data Breach; (d) comply with regulations protecting the PII at issue during the period of the Data Breach; and (e) disclose in a timely and adequate manner that Plaintiff's and the Class Members' PII in

Defendant's possession had been or was reasonably believed to have been, stolen or compromised.

80. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII would not have been compromised.

81. Defendant's failure to take proper security measures to protect the sensitive PII of Plaintiff and Class Members created conditions conducive to a foreseeable, intentional act, namely the unauthorized access of Plaintiff's and Class Members' PII.

82. Plaintiff and Class Members were foreseeable victims of Defendant's inadequate data security practices, and it was also foreseeable that Defendant's failure to provide timely and adequate notice of the Data Breach would result in injury to Plaintiff and Class Members as described in this Complaint.

83. Plaintiff and the Class Members were (and continue to be) damaged as a direct and proximate result of Defendant's failure to secure and protect their Private Information.

84. Defendant's wrongful actions and/or inaction (as described above) constituted, and continue to constitute, negligence at common law.

COUNT II – BREACH OF CONFIDENCE
(ON BEHALF OF PLAINTIFF AND THE CLASSES)

85. Plaintiff re-alleges the preceding paragraphs as is set forth fully in this Count.

86. Plaintiff and Class Members maintained a confidential relationship with Defendant whereby Defendant undertook a duty not to disclose to unauthorized

parties the Plaintiff's and Class Members' PII to unauthorized third parties. Such PII was confidential and novel, highly personal and sensitive, and not generally known.

87. Defendant knew Plaintiff's and Class Members' PII was being disclosed in confidence and understood the confidence was to be maintained, including by expressly and implicitly agreeing to protect the confidentiality and security of the PII they collected, stored, and maintained.

88. As a result of the Data Breach, there was an unauthorized disclosure of Plaintiff's and Class Members' PII in violation of this understanding. The unauthorized disclosure occurred because Defendant failed to implement and maintain reasonable safeguards to protect the PII in its possession and failed to comply with industry-standard data security practices.

89. Plaintiff and Class Members were harmed by way of an unconsented disclosure of their confidential information to an unauthorized third party.

90. But for TIAA's disclosure of Plaintiff's and Class Members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties.

91. The Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' PII, as well as the resulting damages.

92. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' PII.

93. Defendant knew its computer systems and technologies for accepting, securing, and storing Plaintiff's and Class Members' PII had serious security vulnerabilities because it failed to observe standard security practices or correct known security vulnerabilities.

94. As a direct and proximate result of Defendant's violations, Plaintiff and the Class have suffered and continue to suffer injury.

COUNT III - INVASION OF PRIVACY BY PUBLIC DISCLOSURE OF PRIVATE FACTS AND INTRUSION UPON SECLUSION

(ON BEHALF OF PLAINTIFF AND THE CLASSES)

95. Plaintiff re-alleges the preceding paragraphs as is set forth fully in this Count.

96. Plaintiff's and Class Members' Private Information is and always has been private and confidential.

97. Dissemination of Plaintiff's and Class Members' Private Information is not of a legitimate public concern; publication to third parties of their Private Information would be, is and will continue to be, offensive to Plaintiff, Class Members, and other reasonable people.

98. By failing to keep Plaintiff's and Class Members' PII secure, and disclosing PII to unauthorized parties for unauthorized use, TIAA's unlawfully invaded Plaintiff's and Class Members' privacy right to seclusion by, inter alia:

A. Intruding into their private affairs in a manner that would be highly offensive to a reasonable person;

B. Invading their privacy by improperly using their PII properly obtained for specific purpose for another purpose, or disclosing it to unauthorized persons;

C. Failing to adequately secure their PII from disclosure to unauthorized persons; and

D. Enabling the disclosure of their PII without consent.

99. TIAA's wrongful actions and/or inaction (as described above) constituted, and continue to constitute, an invasion of Plaintiff's and Class Members' privacy by publicly disclosing their Private Information.

100. Defendant's instructions were substantial and would be highly offensive to a reasonable person, constituting an egregious breach of social norms.

101. Plaintiff and the Class Members were (and continue to be) damaged as a direct and proximate result of Defendant's invasion of their privacy by publicly disclosing their Private Information, for which they suffered loss and are entitled to compensation.

102. As a direct and proximate result of Defendant's violations, Plaintiff and the Class have suffered and continue to suffer injury.

COUNT IV - BREACH OF CONTRACT

(ON BEHALF OF PLAINTIFF AND THE CLASSES)

103. Plaintiff re-allege the preceding paragraphs as is set forth fully in this Count.

104. Plaintiff and other Class Members entered into valid and enforceable express contracts with Defendant under which Plaintiff and other Class Members agreed to provide their Private Information to Defendant, and Defendant impliedly, if not explicitly, agreed to protect Plaintiff's and Class Members' Private Information.

105. To the extent Defendant's obligation to protect Plaintiff's and other Class Members' Private Information was not explicit in those express contracts, the express contracts included implied terms requiring Defendant to implement data security adequate to safeguard and protect the confidentiality of Plaintiff's and other Class Members' Private Information, including in accordance with federal, state and local laws, regulations, and industry standards. Neither Plaintiff nor any Class member would have entered into these contracts with Defendant without the understanding that Plaintiff's and other Class Members' Private Information would be safeguarded and protected; stated otherwise, data security was an essential implied term of the parties' express contracts.

106. A meeting of the minds occurred, as Plaintiff and Class Members agreed, among other things, to provide their Private Information in exchange for Defendant's agreement to protect the confidentiality of that Private Information.

107. The protection of Plaintiff's and Class Members' Private Information was a material aspect of Plaintiff's and Class Members' contracts with Defendant.

108. Plaintiff and Class Members fully performed their obligations under the implied contract with Defendant; however, Defendant did not.

109. As a result of Defendant's breach of these terms, Plaintiff and Class Members have suffered a variety of damages including but not limited to: the lost value of their privacy; not getting the benefit of their bargain with Defendant; the lost difference in the value between the secure services Defendant promised and the insecure services received; the value of the lost time and effort required to mitigate the actual and potential impact of the data breach on their lives.

110. Additionally, Plaintiff and Class Members suffered emotional distress and diminution in the value of their information since their Private Information was unlawfully shared, and likely continues to reside in the possession of, third parties without their consent. Plaintiff and Class Members have been put at an increased risk of future identity theft, fraud, and/or misuse of their Private Information, which may take years to manifest, discover, and detect.

111. Plaintiff and Class Members are therefore entitled to damages.

COUNT V - BREACH OF IMPLIED CONTRACT

(ON BEHALF OF PLAINTIFF AND THE CLASSES)

(IN ALTERNATIVE TO COUNT IV)

112. Plaintiff re-allege the preceding paragraphs as is set forth fully in this Count.

113. At all relevant times, Defendant had a duty, or undertook and/or assumed a duty, to implement a reasonable data privacy and cybersecurity protocol, including adequate prevention, detection, and notification procedures, in order to

safeguard the Private Information of Plaintiff and the Class members, and to prevent the unauthorized access to and disclosures of this data.

114. Among other things, Plaintiff and Class Members were required to disclose their Private Information to Defendant for the provision of services, as well as implied contracts for the Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

115. When Plaintiff and Class Members provided their Private Information to Defendant in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

116. By entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

117. Under implied contracts, Defendant and/or their affiliated providers promised and were obligated to protect Plaintiff's and Class Members' Private Information. In exchange, Plaintiff and Members of the Class agreed to turn over their Private Information.

118. The implied contracts that include the contractual obligations to maintain the privacy of Plaintiff's and Class Members' Private Information, are also acknowledged, memorialized, and embodied in multiple documents, including (among

other documents) Defendant's data breach notification and Defendant's notices of privacy practices.

119. Defendant's express representations, including, but not limited to the express representations found in their notices of privacy practices, memorialize and embody the implied contractual obligations requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

120. Plaintiff and Class Members performed their obligations under the contract when they provided their Private Information in consideration for Defendant's goods and/or services.

121. Defendant materially breached their contractual obligations to protect the private information Defendant gathered when the information was accessed and exfiltrated during the data breach.

122. Defendant materially breached the terms of the implied contracts, including, but not limited to, the terms stated in the relevant notices of privacy practices. Defendant did not maintain the privacy of Plaintiff's and Class Members' Private Information as evidenced by their notification of the data breach to Plaintiff and Class Members.

123. The data breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

124. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiff and Class Members did not receive full benefit

of the bargain they entered into, and instead received services that were of a diminished value to that described in the contracts. Plaintiff and Class Members, therefore, were damaged in an amount at least equal to the difference in the value between the secure services Defendant promised and the insecure services received.

125. Had Defendant disclosed that their security was inadequate or that they did not adhere to industry-standard security measures, neither Plaintiff, Class Members, nor any reasonable person would have entered into the aforementioned contracts with Defendant.

126. As a direct and proximate result of the data breach, Plaintiff and Class Members have been harmed and suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, out of pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

COUNT VI– UNJUST ENRICHMENT

(ON BEHALF OF PLAINTIFF AND THE CLASSES)

127. Plaintiff re-allege the preceding paragraphs as is set forth fully in this Count.

128. Plaintiff and Class Members have an interest, both equitable and legal, in the PII about them that was conferred upon, collected by, and maintained by Defendant and that was ultimately stolen in the Data Breach.

129. Defendant benefitted by the conferral upon it of the PII pertaining to Plaintiff and Class Members and by its ability to retain, use, sell, and profit from that information.

130. But for Defendant's willingness and commitment to maintain its privacy and confidentiality, that PII would not have been transferred to and entrusted with them.

131. Because of the Defendant's use of Plaintiff's and Class Members' PII, Defendant obtained an economic benefit over and above what it otherwise would have. Defendant was unjustly enriched by profiting from the additional services and products it was able to market, sell, and create to the detriment of Plaintiff and Class Members.

132. Defendant also benefitted through their unjust conduct by retaining money that it should have used to provide reasonable and adequate data security to protect Plaintiff's and Class Members' PII, as well as profits it gained through the use of Plaintiff's and Class Members' PII.

133. It is inequitable for Defendant to retain these benefits.

134. Defendant's retention of wrongfully obtained monies would violate fundamental principles of justice, equity, and good conscience.

135. The benefit conferred upon, received, and enjoyed by Defendant was not conferred officiously or gratuitously, and it would be inequitable, unfair, and unjust for Defendant to retain the benefit.

136. Defendant's defective security and its unfair and deceptive conduct have, among other things, caused Plaintiff and Class Members to unfairly incur substantial time and/or costs to mitigate and monitor the use of their PII and has caused the Plaintiff and Class Members other damages as described herein.

137. Defendant is therefore liable to Plaintiff and Class Members for restitution or disgorgement in the amount of the benefit conferred to it as a result of its wrongful conduct, including specifically: the value to Defendant of the PII that was stolen in the Data Breach; the profits Defendant received and is receiving from the use of that information; the amounts that Defendant overcharged Plaintiff and Class Members for use of Defendant's products and services; and the amounts that Defendant should have spent to provide reasonable and adequate data security to protect Plaintiff's and Class Members' PII.

COUNT VII – DECLARATORY JUDGMENT/INJUNCTIVE RELIEF

(ON BEHALF OF PLAINTIFF AND THE CLASSES)

138. Plaintiff re-allege the preceding paragraphs as is set forth fully in this Count.

139. This Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

140. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to

reasonably safeguard Plaintiff's and Class members' PII, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class members from future data breaches that compromise their PII.

141. Plaintiff and the Class remain at imminent risk that further compromises of their PII will occur in the future.

142. The Court should also issue prospective injunctive relief requiring Defendant to employ adequate security practices consistent with law and industry standards to protect employees' PII.

143. Defendant still possesses the PII of Plaintiff and the Class

144. To Plaintiff's knowledge, Defendant has made no changes to its data storage or security practices relating to the PII.

145. To Plaintiff's knowledge, Defendant has made no announcement or notification that it has remedied any and all vulnerabilities and negligent data security practices that led to the Data Breach.

146. Pursuant to its authority, this Court should enter a judgment declaring, among other things, the following:

A. Defendant continues to owe a legal duty to secure consumers' PII and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes;

B. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII.

C. Engaging third-party security auditors/penetration testers, as well as internal security personnel, to conduct testing that includes simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

D. Engaging third-party security auditors and internal personnel to run automated security monitoring;

E. Auditing, testing, and training its security personnel regarding any new or modified procedures;

F. Purging, deleting, and destroying PII not necessary for its provisions of services in a reasonably secure manner;

G. Conducting regular database scans and security checks; and

H. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

147. The Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect consumers' PII.

148. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach. The risk of another such breach is real, immediate, and substantial.

149. The hardship to Plaintiff and Class members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs at Defendant, Plaintiff and Class members will likely continue to be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

150. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach by Defendant, thus eliminating the additional injuries that would result to Plaintiff and Class members, along with other employees whose PII would be further compromised.

COUNT VIII - VIOLATION OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT, 815 ILCS 505/1, *ET SEQ.*

(ON BEHALF OF PLAINTIFF AND THE ILLINOIS SUBCLASS)

151. Plaintiff re-alleges the preceding paragraphs as is set forth fully in this Count.

152. Section 2 of ICFA prohibits unfair or deceptive acts or practices and states, in relevant part, as follows:

> **Unfair methods of competition and unfair or deceptive acts or practices, including but not limited to the use or employment of any deception, fraud, false pretense, false promise, misrepresentation or the concealment, suppression or omission of such material fact, or the use or employment of any practice described in section 2 of the "Uniform Deceptive Trade Practices Act", approved August 5, 1965, in the conduct of any trade or commerce are hereby declared**

unlawful whether any person has in fact been misled, deceived or damaged thereby.

153. Defendant violated Section 2 of ICFA by engaging in unfair acts in the course of conduct involving trade or commerce when dealing with Plaintiff.

154. Specifically, it was an unfair act and practice to represent to the public that it implemented commercially reasonable measures to protect their PII, Defendant nonetheless failed to fulfill such representations, including by failing to timely detect the Data Breach.

155. Despite representing to Plaintiff and the Illinois Subclass members that it would implement commercially reasonable measures to protect their PII, Defendant nonetheless failed to fulfill such representations.

156. Plaintiff and the Illinois Subclass members have suffered injury in fact and actual damages, as alleged herein, as a result of Defendant's unlawful conduct and violations of the ICFA and analogous state statutes.

157. Defendant's conduct offends public policy as it demonstrates a practice of unfair and deceptive business practices in failing to safeguard consumers PII.

158. An award of punitive damages is appropriate because Defendant's conduct described above was outrageous, willful and wanton, showed a reckless disregard for the rights of the Plaintiff and consumers, generally, and Plaintiff had no choice but to submit to Defendant's illegal conduct.

COUNT IX - VIOLATION OF THE ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT, 815 Ill. Comp. Stat. §§ 510/2, ET SEQ.

(ON BEHALF OF PLAINTIFF AND THE ILLINOIS SUBCLASS)

159. An award of punitive damages is appropriate because Defendant's conduct described above was outrageous, willful and wanton, showed a reckless disregard for the rights of the Plaintiff and consumers, generally, and Plaintiff had no choice but to submit to Defendant's illegal conduct.

160. Plaintiff re-alleges the preceding paragraphs as is set forth fully in this Count.

161. Defendant is a "person" as defined by 815 Ill. Comp. Stat. §§ 510/1(5).

162. Defendant engaged in deceptive trade practices in the conduct of its business, in violation of 815 Ill. Comp. Stat. §§ 510/2(a), including, but not limited to:

A. Representing that goods or services have characteristics that they do not have;

B. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

C. Advertising goods or services with intent not to sell them as advertised; and

D. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

163. Defendant's deceptive acts and practices include:

A. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's Private Information, which was a direct and proximate cause of the Data Breach;

B. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

C. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's Private Information, which was a direct and proximate cause of the Data Breach;

D. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff's Private Information, including by implementing and maintaining reasonable security measures;

E. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's Private Information;

F. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's Private Information; and

G. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's Private Information, including

duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

164. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of its data security and ability to protect the confidentiality of consumers' Private Information.

165. The above unfair and deceptive practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

166. As a direct and proximate result of Defendant's unfair, unlawful, and deceptive trade practices, Plaintiff has suffered and will continue to suffer injury.

167. Plaintiff and the Illinois Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorney's fees and costs.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff ask for an award in their favor and against Defendant as follows:

A. Certifying this action as a class action, with a class as defined above;

B. Designation of Plaintiff as representatives of the proposed Class and designation of Plaintiff's counsel as Class counsel;

C. For equitable and injunctive relief enjoining Defendant from engaging in the wrongful acts and omissions complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private

Information, and from failing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

D. Awarding compensatory and actual damages to redress the harm caused to Plaintiff and Class Members;

E. Awarding punitive damages as allowable by law;

F. Awarding Plaintiff and the Class Members interest, costs and attorneys' fees;

G. Such other and further relief as this Court deems just and proper.

Respectfully Submitted,

By: /s/ *Bryan Paul Thompson*
One of Plaintiff's Attorneys

Bryan Paul Thompson
Robert W. Harrer
CHICAGO CONSUMER LAW CENTER, P.C.
650 Warrenville Road, Suite 100
Lisle, IL 60532
Tel. 312-858-3239
Fax 312-610-5646
bryan.thompson@cclc-law.com
rob.harrer@cclc-law.com

DOCUMENT PRESERVATION DEMAND

Plaintiff hereby demands that defendant take affirmative steps to preserve all recordings, data, documents, and all other tangible things that relate to plaintiff, the events described herein, any third party associated with any telephone call, campaign, account, sale or file associated with plaintiff, and any account or number or symbol relating to them. These materials are likely very relevant to the litigation of this claim. If defendant is aware of any third party that has possession, custody, or control of any such materials, Plaintiff demands that defendant request that such third party also take steps to preserve the materials. This demand shall not narrow the scope of any independent document preservation duties of the defendant.

By: /s/ *Bryan Paul Thompson*
One of Plaintiff's Attorneys